Cisco Connected Grid Modules for CGR 1000 Series—WiMAX Installation and Configuration Guide

First Published: September 2012
Last Updated: June 2013
OL-26236-03

This document provides an overview of hardware and configuration information for Cisco Connected Grid Modules for CGR 1000 Series—WiMAX.

The WiMAX module provides the Wide-Area Network (WAN) connection for critical data applications in supporting the Connected-Grid Router (CGR) as a backup data link for critical data applications.

This document contains the following topics:

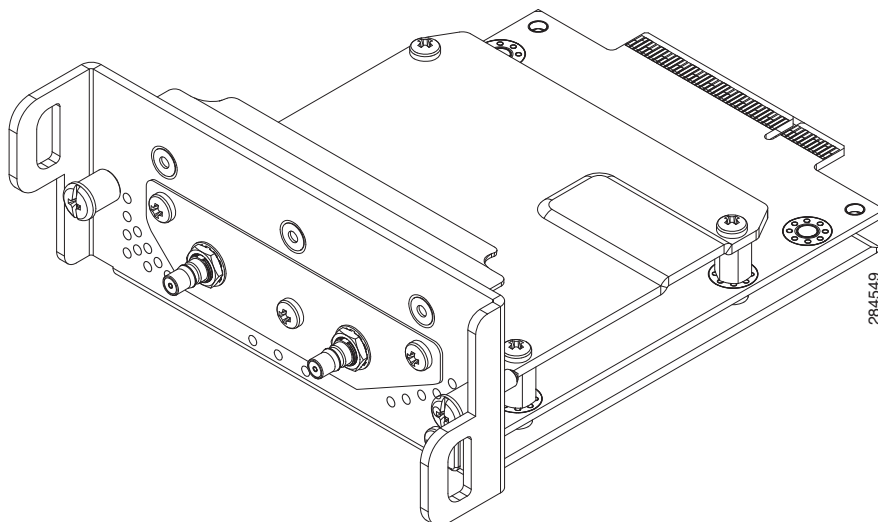⚠️ **Warning** **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Cisco Systems, Inc.
www.cisco.com

Figure 1   *Cisco Connected Grid Modules for CGR 1000 Series—WiMAX*

Parts List

Your WiMAX module kit contains one the following WiMAX radio modules. Parts can be ordered by referencing the following information shown in Table 1:

Table 1   *Kit Contents for WiMAX module*

Cisco Part Number	Description
CGM-WIMAX-1.8	WiMAX 1.8 GHz band, subscriber station radio module
CGM-WIMAX-2.3	WiMAX 2.3 GHz band, subscriber station radio module
CAB-L240-10-Q-N	Internal cable, RA-QMA(m) to N(m), LMR-240-FR, 10', quantity 1
CAB-L100-17-Q-M	Internal cable, RA-QMA(m) to RA-MCX (m), LMR-100, 17.5", quantity 2
CAB-L400-20-N-N	Outdoor cable, RA-N(m)-N(m), LMR-400-DB, 20', quantity 2
CAB-L600-30-N-N	Outdoor cable, RA-N(m)-N(m), LMR-600-DB, 30', quantity 2
CGR-LA-NF-NF	Lightning arrestor, N(f)-N(f), quantity 2
ANT-1.8-PNL-OUT-N	Flat-panel antenna, 1800 to 1830 MHz, 15 dBi, N(f), dual-slant, quantity 1
ANT-2.X-PNL-OUT-N	Flat-panel antenna, 2.3 to 2.7 GHz, 17 dBi, N(f), dual-slant, quantity 1
CGR-LA-NM-NF	Bulkhead adapter, MCX(f) receptacle, N(f), quantity 2 and lightning arrestor, DC Pass, N(m)-N(f), quantity 2
CGR-N-CONN-WIMAX	N-connector kit: LMR-400 cable, weather-proof cap, coaxial seal, electrical-joint compound (used with external antennas and WiMAX module)

For system requirements, important notes, limitations, open and resolved bugs, and last-minute documentation updates, see the Release Notes on Cisco.com. For translations of the warnings that appear in this document, see the *Regulatory Compliance and Safety Information* document for your router on Cisco.com.

When using the online publications, see the documents that match the Cisco system software version running on the wireless module.

Features

Cisco Connected Grid Modules for CGR 1000 Series—WiMAX offers the following key features:

Table 2   Feature Information for WiMAX module

Feature	Description
WiMAX technology standard	IEEE 802.16e
Bands	1.4 GHz band: 1390 to 1510 MGhz (CGM-WIMAX-1.4GHz) 1.8 GHz band: 1800 to 1830 MHz (CGM-WIMAX-1.8GHz) 2.3 GHz bands: 2300 to 2360 MHz (CGM-WIMAX-2.3GHz) 3.65 GHz bands: 3300 to 3800 MHz (CGM-WIMAX-3.65GHz) ✎ **Note** The WiMAX module is capable of operation in the listed frequency band and its hardware can be configured for operation in one band at a time by way of circuit board assembly option.
Mobile Broadband Wireless Access System	IEEE 802.16e-2009
Two antenna ports	50 ohms impedance, QMA connector (jack).
Operation mode	TDD (Time Division Duplex)
Channel bandwidth	3.5, 5.0, 7.0, and 10 MHz
Number of transmitters	2
Number of receivers	2 (MRC and CL-MIMO)
Maximum transmit power	23 dBm per transmit stream, 2 streams
Security	• PkmV2 • Authentication: EAP-TLS and EAP-TTLS • Digital certificate
Data rates	• The actual throughput rates depends on many different factors, but the theoretical rates for the technologies follows: • Mobile WiMAX technology to support peak DL data rates up to 63 Mbps per sector and peak UL data rates up to 28 Mbps per sector in a 10 MHz channel.
Authentication	Hash-based Message Authentication Code (HMAC) and Cipher-based MAC (CMAC) support.
Module management	Enables you to access modem software and hardware information, radio and network status, and data profile information by using Cisco commands.
Antenna	Multiple antenna and cable options: • Separate dual antennas or dual-polarized antenna • Chassis integrated and outdoor externally mounted antennas • Radio Frequency Ultra-Low Loss (RF-ULL) coaxial cable

Table 2   Feature Information for WiMAX module (continued)

Feature	Description
WiMAX IP and Ethernet Convergence Sublayer	Allows a WiMAX network to provide Ethernet service directly to customers.
Frequency resolution	0.25 MHz
Antenna connectors	1 pair of antenna connectors; 50 ohms; QMA female (jack)
Antenna diversity support	1x2 STC/MIMO-SM [Matrix A], or 2x2 STC/MIMO-SM [Matrix B]
Linear output transmit power (average power):	One of the following: • 23 dBm, maximum, one spatial stream at room temperature • 23 dBm, maximum, each, two spatial streams
Transmit power control range	10 dB minimum
Modulation/coding	• Support all configuration defined in WiMAX system profile 1.0 for DL up to QAM 64 5 /6 • Support all configuration defined in WiMAX system profile 1.0 for UL up to QAM 64 5 /6
Linear output power	The module supports up to 23 dBm nominal per spatial stream at room temperature
Forward Error Correction Code (FEC)	• CC (Convolutional Codes)—1/2 to 3/4 • CTC (Convolutional Turbo Codes)—1/2 to 5/6
Dynamic range	• Tx dynamic range: 43 dB (-20 dBm to 23 dBm) • Rx dynamic range: 70 dB (-100 dBm to -30 dBm)
Mean time before failure (MTBF)	Calculate in accordance with Telecordia SR332

Hardware Overview

The WiMAX module is designed to be installed into the CGR 1000 Series Routers ruggedized routers/concentrators designed for deployments in secondary substations within the electric utility distribution grid. The WiMAX module is used mainly for uplink to the Neighborhood Area Network (NAN) within the Smart Grid environment.

The main function of the WiMAX module is the WAN uplink over wireless 2.3GHz band in Distribution Automation and AMI concentrator deployment. The WiMAX module runs on CG-OS.

This section covers the following topics:

- Temperature Monitoring State Machine, page 10
- Module Power States, page 10

Front Panel

Figure 2 shows the front panel components of the WiMAX module.

Figure 2   *Front Panel of the WiMAX Module*
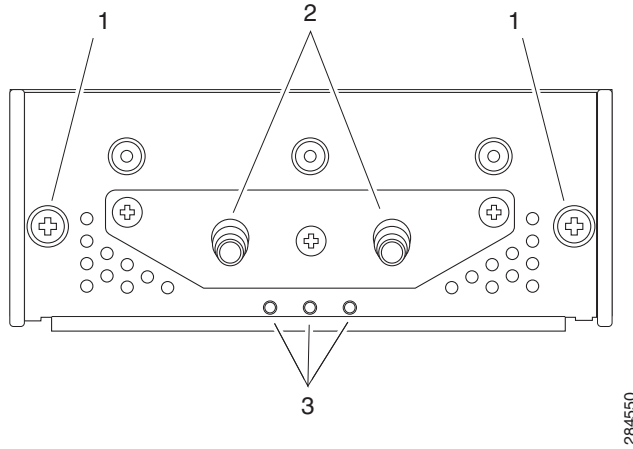
1	Captive screws (2)	2	QMA(f) connector (2)
3	LEDs (WWAN, SVC, RSSI)		

Supported Cisco WiMAX Antennas

The antenna is connected to the QMA, panel-mount, 50-ohm connector located on the faceplate of the module.

For more information about antennas, including installation procedures, see *Cisco 1240 and 1120 Connected Grid Router Hardware Installation Guide.*

Table 3 lists the Cisco antennas that are supported for use with the module and the Cisco 1240 Connected Grid Router.

Table 3 **CGR 1240—Supported Antennas and Cables for the WiMAX Module**

Cisco 1240 Connected Grid Router				
Case Description	**Internal Cable**	**Adapter or Lightning Arrestor**	**Outdoor Cable**	**Antenna**
WiMAX 1.4 GHz external antenna	(2) LMR-100, 17.5", 37-1380-01, CAB-L100-17-Q-M	• (2) N Bulkhead Adapters, 29-5950-01 • (2) Lightning Arrestors, 07-1091-01, CGR-LA-NM-NF	(2) LMR-400-DB, 20', 37-1392-01, CAB-L400-20-N-N	(1) Flat-panel antenna, 1390-1465 MHz, 13 dBi, dual slant, 07-1218-01, ANT-1.4-PNL-OUT-N
WiMAX 1.4 GHz integrated antenna	(2) LMR-100, 17.5", 37-1380-01, CAB-L100-17-Q-M	—	—	(2) Monopole antennas, 1350-1525 MHz, chassis mounted, omnidirectional, 07-1140-02, ANT-WM-INT-OUT-M
WiMAX 1.8 GHz external antenna	(2) LMR-100, 17.5"', 37-1380-01, CAB-L100-17-Q-M	• (2) N Bulkhead Adapters, 29-5950-01 • (2) Lightning Arrestors, 07-1091-01, CGR-LA-NM-NF	• (2) LMR-400-DB, 20' CAB-L400-20-N-N • (2) LMR-600B-DB, 30', CAB-L600-30-N-N	(1) Flat-panel antenna, 1800-1830 MHz, 15 dBi, dual slant, 07-1159-01, ANT-1.8-PNL-OUT-N
WiMAX 1.8 GHz integrated antenna	(2) LMR-100, 17.5", 37-1380-01, CAB-L100-17-Q-M	—	—	(2) Integrated antennas, 07-1140-02
WiMAX 2.3GHz external Antenna	(2) LMR-100, 17.5", 37-1380-01, CAB-L100-17-Q-M	• (2) N Bulkhead Adapters, 29-5950-01 • (2) Lightning Arrestors, 07-1091-01, CGR-LA-NM-NF	• (2) LMR-400-DB, 20' CAB-L400-20-N-N • (2) LMR-600B-DB, 30' CAB-L600-30-N-N	(1) Flat-panel antenna, 2300-2700 MHz, 17 dBi, dual slant, 07-1160-01, ANT-2.X-PNL-OUT-N
WiMAX 2.3 GHz integrated antenna	(2) LMR-100, 17.5", 37-1380-01, CAB-L100-17-Q-M	—	—	(2) Integrated antennas, 07-1140-02

Table 3   *CGR 1240—Supported Antennas and Cables for the WiMAX Module*

	Cisco 1240 Connected Grid Router			
Case Description	Internal Cable	Adapter or Lightning Arrestor	Outdoor Cable	Antenna
WiMAX 3.65 GHz external antenna	(2) LMR-100, 17.5", 37-1380-01, CAB-L100-17-Q-M	• (2) N Bulkhead Adapters, 29-5950-01 • (2) Lightning Arrestors, 07-1091-01, CGR-LA-NM-NF	• LMR-400-DB, 20' CAB-L400-20-N-N • LMR-600B-DB, 30' CAB-L600-30-N-N	(1) Flat-panel antenna, 3300-3800 MHz, 18.5 dBi, dual slant, 07-1161-01, ANT-3.X-PNL-OUT-N
WiMAX 3.65 GHz integrated antenna	(2) LMR-100, 17.5", 37-1380-01, CAB-L100-17-Q-M	—	—	(2) Monopole antennas, 3300-3800 MHz, chassis mounted, omnidirectional, 07-1142-02, ANT-WM-INT-OUT-M

Mechanical Specifications

The following are the mechanical specifications of the WiMAX module.

Table 4   *Mechanical, Power, Environmental Standards*

Feature	Description
Operating temperature of the CGR 1240 (WiMAX module installed)	-40 to 158-degrees F (-40 to 70-degrees C)
Power consumption	• 8 W maximum over temperature • 12 V DC +/- 5% (+/- .6 V) • 3.3V DC +/- 5% (+/- .6 V) average (with 70% Tx duty cycle)
EMC	FCC Part 15, Subpart B, Class B
Radio	• Industry Canada SRSP-301.7 for 1.8 GHz • FCC Part 27 for 2.3 GHz • FCC Part 90Z for 3.65 to 3.7 GHz

WiMAX Interface

The WiMAX module performs the following responsibilities:

• Transmitting the receiving data packets

• Controlling and configuring WiMAX radio and Media Access Control (MAC) parameters

• Collecting statistics from radio

• Process alarms

• Registering and authenticating with the WiMAX network

• Scanning for and choosing the base station (BS)

The module provides two physical connectors for antennas.

Module States

The WiMAX module has the following states:

Table 5 **WiMAX Module States**

State	Description
Configured	In this state the WiMAX module has all the necessary configuration information and can be started by the port manager. Modifications to configuration parameters using the configuration file require re-initialization of the WiMAX module.
	Input signal(s):
	MAC start
	• Action—Starts the MAC process
	• Next state—Disconnected
	Configuration error
	• Action—Send message
	• Next state—Initializing
	This state corresponds to the port manager configured state.
Disconnected	Corresponds to the Interface Down state.
	Exit Criteria: Start of Scanning.
Scanning	This state is internal to the WiMAX module and does not need to be exposed to the port manager other than for debug purposes.
	Exit criteria: BS found or stop scanning signal from the Port manager.
Connecting	This state is internal to the WiMAX module and does not need to be exposed to the port manager other than for debug purposes.
	Exit criteria: finished SBC message exchange.
Authenticating	This state is internal to the WiMAX module and does not need to be exposed to the port manager other than for debug purposes.
Connected	In this state the WiMAX module has at least one SF each in the DL and UL. This SF is called the Initial service flow (ISF). Additional SF may be created by the BS as required.
	This state is exposed to the port manager. The method of exposing this state to the port manager is TBD; need to review the code to determine if there and explicit message or the Module needs to be polled.

Radio Frequency Interface

The Radio Frequency (RF) interface consists of two QMA connectors on the faceplate labeled *MAIN* and *AUX*. Both antennas are mandatory; it both transmits and receives RF. The second *AUX* QMA connector is for the optional RX Diversity.

DC Power Consumption

The average DC power consumption according to the duty cycle is as follows:

Table 6   Power Specifications WiMAX 1.8 MHz Module

Transmit Duty Cycle (Tx/Rx)	1 Transmit Spatial Stream	2 Transmit Spatial Streams
40%/60%	3.7 W	5.3 W

Temperature Monitoring State Machine

The state machine in the WiMAX module monitors the embedded module temperature. The command **show environment temperature** shows the module temperature in Celsius. For example, the temperature sensor of the WIMAX module shows as 46-degrees Celsius.

```
# show module
Mod   Ports   Module-Type                          Model              Status
---   -----   ------------------------------------ ------------------ ----------
1     0       CGR1000 Supervisor Module            CGR1120/K9         active *
2     9       CGR1000 Ethernet Module              CGR1000            ok
3     1       Connected Grid Module - IEEE 802.16  CGM-WIMAX-1.8GHZ   ok
4     1       Connected Grid Module - IEEE 802.15  CGM-WPAN-FSK-NA    ok

# sh environment temperature
Temperature:
----------------------------------------------------------------------
Module   Sensor       MajorThresh   MinorThres   CurTemp     Status
                      (Celsius)     (Celsius)    (Celsius)
----------------------------------------------------------------------
1        Sensor0      75            60           44          Ok
3        Sensor0      75            60           46          Ok
4        Sensor0      75            60           46          Ok
```

Module Power States

The module has the following power states:

- **Normal mode**—Module is active. Receive and Transmit modes are possible. In this state:
  - The module is fully powered.
  - The module is capable of placing/receiving calls or establishing data connections on the wireless network.
  - The USB interface is fully active.

Note   The module unit defaults to the Normal state when VCC is first applied.

- **Disconnected mode**—No power to the module. The host power source is disconnected from the module and all voltages associated with the module are at 0 V.

  CGR 1120 and CGR 1240 controls the power to the module, therefore the host can stay powered on and cut the power in order to put the module into the disconnected state.

Installing and Removing the WiMAX Module

Note   After replacing or installing a module in the router, you must update the label (on the router exterior) that lists the module types contained in the router. The label must list the FCC ID number and the IC Certification number for each module installed in the router.

This section covers the following topics:

Before You Begin Installation

Before installing the module, verify that the following guidelines have been met:

- Clearance to the I/O-side view is such that the LEDs can be easily read.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures. Make sure that the cabling is away from other devices that might damage the cables.
- Airflow around the unit and through the vents is unrestricted.
- Relative humidity around the unit does not exceed 95 percent (non-condensing).
- Altitude at the installation site is not higher than 10,000 feet.
- For 10/100 and 10/100/1000 fixed ports, cable lengths from the unit to connected devices are not longer than 328 feet (100 meters).

Installation Warning Statements

This section includes the basic installation warning statements. Translations of these warning statements appear in the *Regulatory Compliance and Safety Information for Cisco Connected Grid Router 1000 Series Routers* documents.

Warning   **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning   **To prevent airflow restriction, allow clearance around the ventilation openings to be at least: 1.75 in. (4.4 cm)** Statement 1076

Installing the WiMAX Module

The WiMAX module can be installed into any slot of the CGR 1240, however Slot 6 is recommended due to the ease of installing the available cable.

Note   Some WiMAX modules are installed into the host router at the factory.

To install the module into an available slot in the Cisco Connected Grid 1120 Router or the Cisco Connected Grid 1240 Router:

Note   The module can be hot swapped because module online insertion removal (OIR) is allowed—it is not necessary to power down the router.

Step 1   Before you install (or remove) the Connected Grid WiMAX module from the host router, read the instructions about installing and removing modules in the *Hardware Installation Guide* of your router.

Step 2   Insert the WiMAX module in the slot.

Step 3   Using a screwdriver, secure the two captive screws into place.

Removing the WiMAX Module

To remove the WiMAX module from a slot in the Cisco Connected Grid 1120 Router or the Cisco Connected Grid 1240 Router:

Note   The module can be hot swapped because module online insertion removal (OIR) is allowed—it is not necessary to power down the router.

Step 1   Before you remove the Connected Grid WiMAX module from the host router, read the instructions about installing and removing modules in the *Hardware Installation Guide* of your router.

Step 2   Using a screwdriver, loosen the two captive screws on the Connected Grid WiMAX module.

Step 3   Gently pull the WiMAX module out of the slot.

Standards

The following standards apply to the Cisco Connected Grid Modules for CGR 1000 Series—WiMAX.

Table 7   General Standards

Standard	Definition
IEEE 1613 2009	IEEE Standard for Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations

Regulatory and Compliance Information

For regulatory compliance and safety information for the module, refer to the *Connected Grid Router 2000 Series Regulatory Compliance and Safety Information* document.

http://www.cisco.com/en/US/docs/routers/access/2000/CGR2010/hardware/rcsi/rcsiCGR2000series.html

Software Overview

This section covers basic configuration, debugging, and troubleshooting information for the Cisco 1000 Series Connected Grid Router (CGR 1000).

This section provides information on the following:

WiMAX Overview

Worldwide Interoperability for Microwave Access (WiMAX) is a standards-based wireless technology that offers high-throughput broadband connections over long distances. WiMAX can be used for a number of applications, including "last mile" broadband connections, fixed and mobile cellular service, hotspots and cellular backhaul, and high-speed enterprise connectivity for business.

The Cisco Connected Grid Modules for CGR 1000 Series—WiMAX module is based on the IEEE 802.16e standard for mobile wireless.

Cisco Broadband Wireless Access products for Mobile WiMAX feature advanced antenna systems and support adaptive beamforming and multiple-input multiple-output (MIMO). They allow for multi-megabit service delivery, increased coverage, and greater indoor penetration for the following benefits:

- Subscribers experience high-quality wireless services
- Service providers get fewer service calls, faster time-to-market with new services, and improved cost efficiencies

This open-standards solution is compliant with the Mobile WiMAX specification and the Profile C Network Reference Model. It includes a full suite of base stations, antenna systems, access service network gateways, management systems, and customer premises equipment.

For more on the WiMAX technology, see the following:

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_11-2/112_wimax.html

WiMAX Link QoS

QoS is configured on the base station. The IEEE standard 802.16e provides the ability to define Quality of Service (QoS) for different data streams. It contains definitions of available parameters and scheduling types. The responsibility of QoS is split between the base station and the mobile stations. The base station scheduler is in control of managing the overall QoS of the system. However, the mobile station uplink scheduler is responsible for QoS management between service flows allocated to that MS. The base-station scheduler is entirely responsible for the downlink scheduling.

The WIMAX protocol follows the *Request for Connection; Grant for Terminal* model. In this model, the mobile station issues bandwidth requests that indicate the pending demand for each connection. The base station scheduler, using this information, generates an uplink grant (a grant is the time and frequency allocation for uplink transmission). The mobile station uplink scheduler uses this grant to allocate access to the uplink for its service flows based on its local knowledge of service flow priorities. The mobile station uplink scheduler can be configured for different behavior.

WiMAX connections are defined by service flows. Each service flow is described in terms of QoS parameters and policy of allocations. Service flows contain classification rules which assign packets to specified connection.

QoS Support

In the Mobile WiMAX MAC layer, QoS is provided through service flows. This is a unidirectional flow of packets that is provided with a particular set of QoS parameters. Before providing a certain type of data service, the base station and user-terminal first establish a unidirectional logical link between the peer MACs called connection. The outbound MAC then associates packets traversing the MAC interface into a service flow to be delivered over the connection. The QoS parameters associated with the service flow define the transmission ordering and scheduling on the air interface.

The connection-oriented QoS therefore, can provide accurate control over the air interface. Since the air interface is usually the bottleneck, the connection-oriented QoS can effectively enable the end-to-end QoS control. The service flow parameters can be dynamically managed through MAC messages to accommodate the dynamic service demand. The service flow based QoS mechanism applies to both DL and UL to provide improved QoS in both directions. Mobile WiMAX supports a wide range of data services and applications with varied QoS requirements.

QoS Output

The following is sample QoS configuration on a base station:

```
Router(config-if)# show interface wimax 4/1 service-flows brief
sfid          cid bcid     type     state      direction  rules  arq  harq
-------------------------------------------------------------------------
0               3    3     basic    active  Bidirectional     0   NO    NO
0             515    3     primary  active  Bidirectional     0   NO    NO
4294959123   1034    3       data   active       Downlink     0   NO    NO
8007         1045    3       data   active       Downlink     1   NO   YES
8008         1028    3       data   active         Uplink     1   NO   YES
8091         1026    3       data   active       Downlink     1   NO   YES
8092         1040    3       data   active         Uplink     1   NO   YES
```

```
Router(config-if)# show interface wimax 4/1 service-flows sfid 8091

Sfid                  : 8091
CID                   : 1026
Basic CID             : 3
Type                  : data
State                 : active
Direction             : Downlink
SAID                  : 65535
Encryption algorithm  : None
Authentication algorithm : None
Scheduling type       : Best-effort service
Delivery service      : best-effort
QoS set               : Provisioned set
        Traffic priority      : 3
        Max rate              : 30000000
        Max burst             : 1000000
        Min rate              : 0
        Max latency           : 1000
        Tolerated jitter      : 1000
        Grant interval        : 0
        Polling Interval      : 0
QoS set               : Admitted set
        Traffic priority      : 3
        Max rate              : 30000000
        Max burst             : 1000000
        Min rate              : 0
        Max latency           : 1000
        Tolerated jitter      : 1000
        Grant interval        : 0
        Polling Interval      : 0
QoS set               : Active set
        Traffic priority      : 3
        Max rate              : 30000000
        Max burst             : 1000000
        Min rate              : 0
        Max latency           : 1000
        Tolerated jitter      : 1000
        Grant interval        : 0
        Polling InterBROADCAST BWR         : YES
MULTICAST BWR         : YES
PIGGYBACK BWR         : YES
FRAGMENTATION         : YES
PHS                   : NO
PACKING               : NO
CRC                   : YES
FSN                   : 11bit
Convergence sublayer  : 802.3
ARQ                   : NO
HARQ                  : YES
Rules                 : 1
Total received bytes  : 0
Total PDU bytes       : 0
total PDU packets     : 0
total PDU packets dropped : 0
Total SDU Bytes       : 0
Total SDU packets     : 0
Total SDU packets dropped : 0
Total ARQ blocks      : 0
Total ARQ blocks retry : 0
Total ARQ discards    : 0
Total transmit packets sent : 0
Total sync lost       : 0
Uptime                : 5841val        : 0
```

QoS Parameters

The following are configurable QoS parameters available on the base station:

- **Traffic priority**—This parameter defines the priority assigned to specified service flow. Services with higher traffic priority should be given lower delay and higher buffering preference. However this parameter should not take precedence over any other QoS parameters. The specific algorithm for traffic priorities depends on vendor solution. Available values for this parameter: 0-7 (higher value indicates higher priority).

  The standard only provides recommendation with respect to using the traffic priority, but it is not a requirement. T standard is also clear that the scheduler behavior is left for vendors' differentiation and is out of the standards' scope.

- **Maximum sustained traffic rate**—This parameter defines the peak information rate of specified service flow. If rate is undefined or equal 0, then rate is limited by physical capacity and other connections. Specific implementation of this parameter depends on vendor solution. Available values: rate in bits per second (value does not include overhead caused by MAC headers and CRCs).

- **Maximum traffic burst**—This parameter defines the maximum burst size that is accommodated for the specified service flow. Available values: size in bytes.

- **Minimum reserved traffic rate**—This parameter defines the minimum rate reserved for specified service flow. It is in a sense the guaranteed rate. The specified rate shall be honored only when sufficient data is available for scheduling. Available values: bits per second (value does not include overhead caused by MAC headers and CRCs).

- **Request/transmission policy**—This parameter defines specific policy for selected service flow. This policy defines the "shall/shall not" parameters for the following policies:
  - Broadcast bandwidth request opportunities
  - Multicast bandwidth request opportunities
  - Use piggyback requests with data
  - Fragment data
  - Suppress payload headers (CS parameter)
  - Pack multiple service data units (SDUs) into single Media Access Control (MAC) Packet Data Unit (PDU)
  - Include CRC in the MAC PDU.

- **Tolerated jitter**—This parameter defines the maximum delay variation for specified service flow. Available values: jitter in ms.

- **Maximum latency**—This parameter defines the maximum delay between the reception of a packet on network interface and the forwarding of the packet to the RF interface. Available values: delay in ms.

- **Unsolicited grant interval**—This parameter defines the nominal interval between successive data grant opportunities for specified service flow. Available values: interval in ms.

- **Unsolicited polling interval**—This parameter defines the maximal nominal interval between successive polling grants opportunities for specified service flow. Available values: interval in ms.

- **ARQ enable**—This parameter defines that ARQ (automatic repeat request) shall/shall not be used for specified service flow. This functionality is optional and depends on vendor solution. Available values: 0 – disabled, 1 – enabled.

  ARQ must be enabled for all HARQ enabled service flow.

- **CS specification**—This parameter defines convergence sublayer which should be used for this service flow

Additional QoS Commands

- (config-scan-list)# **nap id nap-id priority** *priority* **channel-index** *channel-index*
- (config-scan-list)# **nsp id nsp-id** {**home** | **priority** *priority* **channel-index** *channel-index*}

Configuring the Module

The module is configured using the system software. This section covers the following topics:

- Prerequisites, page 17
- Guidelines and Limitations, page 17
- WiMAX Interface Security, page 18
- Step 1–WiMAX Scan-list Configuration, page 20
- Step 2–WiMAX Interface Configuration, page 20
- Step 3–Enable Security Parameters, page 20
- Enabling an Interface, page 21
- Additional WiMAX Configuration Commands, page 21
- WiMAX show Command Examples, page 21

Prerequisites

The MTU size of the WiMAX module default is set to 1500 bytes. The WiMAX module is configured with a default MTU size of 1500 in order to provide for roaming of a WiMAX mobile device in an IP sub-convergence layer deployment where an access service network gateway (ASN-GW), such as a Cisco ASR 5000, is used. However, when an MTU size of 1500 bytes is configured on an Ethernet interface such as in a sub-convergence deployment of a private WiMAX infrastructure that also runs Distribution Automation as Ethernet Layer 2 traffic (as for a utility company), then it is possible that OSPFv2 adjacency goes down due to the WiMAX MTU size not matching that of the Ethernet.

Guidelines and Limitations

The following guidelines and limitations apply to configuring the WiMAX module:

- Data connection can be originated only by the module.
- Throughput: Due to the shared nature of wireless communications, the experienced throughput varies depending on the number of active users or congestion in a given network.
- Any restrictions that are a part of the terms of service from your carrier.

- When a WiMAX module operates in a network with an Airspan base station that has a MAC profile definition based on non-authentication, some of its base station models might require the privacy key management (PKM) to be configured on the WiMAX interface. Updating the base station with the latest firmware generally eliminates the need to change the configuration of the WiMAX module.

WiMAX Interface Security

The WiMAX module supports the following security methods:

- IEEE 802.16—WiMAX interface Privacy Key Management v2 authentication.
- EAP-TLS—Extensible Authentication Protocol Transport Layer Security (RFC 5216), 802.1x.
- EAP TTLS—Tunneled Transport Layer Security (RFC 3748).
    - MS-CHAPv2—Challenge-Handshake Authentication Protocol Version 2 (RFC 2759).

> **Note** You must complete WiMAX scanlist configuration before attempting the WIMAX interface configuration. Without associating the WIMAX interface with a configured WIMAX scanlist, you cannot issue a security command on the WIMAX interface since the interface needs to be associated with a WiMAX scanlist first.

To configure security on the WiMAX module, complete the following in this order:

Step 1 Configure the WiMAX scanlist. See Step 1–WiMAX Scan-list Configuration, page 20.

Step 2 Associate the WiMAX scanlist to the WiMAX interface. See Step 2–WiMAX Interface Configuration, page 20.

Step 3 Configure the IP address (static or DHCP) for the WiMAX interface. See Step 2–WiMAX Interface Configuration, page 20.

Step 4 If you want to configure EAP-TLS or EAL-TTLS as your WiMAX authentication method, then you must configure the certificate trustpoints. See Step 3–Enable Security Parameters, page 20.

Step 5 Configure EAP TLS or EAP-TTLS. See Step 3–Enable Security Parameters, page 20.

> **Note** The command **pkm crypto algorithm aes** does not need to be configured since it was included as the default configuration for the WIMAX interface.

WiMAX X.509 Certificates

Learn more about WiMAX Forum X.509 certificates, see http://www.wimaxforum.org.

EAP-TLS and EAP-TTLS Authentication Methods

To set up a username and password for the Pairwise Key Management (PKM) of a CGR 1000, the WiMAX module must be installed and running. CGR 1000s that ship with a pre-installed WIMAX module will have a pre-installed WiMAX configuration.

You can configure your WiMAX interface for one of the following authentication methods:

- **No Authentication** (Open)

- **EAP-TLS Authentication**

  The WiMAX interface uses trustpoints in the following manner. A certificate-based mutual authentication is mandatory. The WiMAX module needs both of the following for authentication:

  – A server-root-ca CA certificate authority trustpoint containing the CA certificate that signs the certificate being used on the AAA/RADIUS server.

  – A device trustpoint for the WIMAX module. The modem on the WiMAX module has an embedded Airspan-signed device certificate that the supplicant can automatically use as the device trustpoint for authentication. If users do not want to use this certificate, they must import and specify a device trustpoint using the imported device certificate.

  – To configure EAP-TLS to use a user-defined WIMAX device certificate:

    ```
    Router(config-if)# shutdown
    Router(config-if)# pkm version pkm-v2
    Router(config-if)# pkm trustpoint device actual_device_trustpoint_label
    Router(config-if)# pkm trustpoint server-root-ca actual_ca_trustpoint_label
    Router(config-if)# pkm auth-method eap-tls
    Router(config-if)# no shutdown
    ```

  – To configure EAP-TLS to use the embedded Airspan certificate as the WIMAX device certificate:

    ```
    Router(config-if)# shutdown
    Router(config-if)# pkm version pkm-v2
    Router(config-if)# pkm trustpoint server-root-ca actual_ca_trustpoint_label
    Router(config-if)# pkm auth-method eap-tls
    Router(config-if)# no shutdown
    ```

  If the trustpoint CLI is not issued for device trustpoint, then the system uses the embedded certificate.

- **EAP-TTLS Authentication**

  EAP-TTLS authentication is a one-sided authentication using an Airspan certificate. A certificate-based authentication is only required for the AAA/RADIUS server. Only a server-root-ca trustpoint configuration is required for the WIMAX interface to authenticate the AAA/RADIUS server certificate. The client (WIMAX interface) authentication is executed through MSCHAPv2 authentication (configuring the PKM user and password) through an encrypted tunnel.

    ```
    Router(config-if)# shutdown
    Router(config-if)# pkm version pkm-v2
    Router(config-if)# pkm trustpoint server-root-ca actual_ca_trustpoint_label
    Router(config-if)# pkm username actual_user_name password actual_password
    Router(config-if)# pkm auth-method eap-ttls
    ```

Step 1–WiMAX Scan-list Configuration

To create a scan-list, issue the following commands:

```
Router# configure terminal
Router(config)# wimax scan-list aaa
Router(config-scan-list)# channel index 1 frequency 2350000 bandwidth 10000
Router(config-scan-list)# nap id 00:00:01 priority 1 channel-index 1
Router(config-scan-list)# nsp id 00:00:01 home
```

- NAP (Network Access Provider)—The base station. It provides access to the NSPs which provides network connectivity.

- NSP (Network Service Provider)—Provides network connectivity and access to NAPs.

- Maximum number of the number of frequencies: 1

Step 2–WiMAX Interface Configuration

To attach the scan-list to an interface, issue the following commands:

```
Router# configure terminal
Router(config)# interface wimax interface_name
Router(config-if)# no shutdown <-- THIS SHOULD BE SHUT
Router(config-if)# scan-list aaa
Router(config-if)# ip address dhcp
Router(config-if)# no shutdown
```

Step 3–Enable Security Parameters

To enable security parameters, follow these steps:

Step 1 Load the certificates onto the bootflash. Create a trustpoint and import the device certificate.

```
Router# configure terminal
Router(config)# crypto ca trustpoint device_cert_trustpoint
Router(config)# crypto ca import device_cert_trustpoint pkcs12 path password
```

Step 2 Create a trustpoint and import the server root certificate authority (CA) certificate.

```
Router(config)# crypto ca trustpoint server_root_CA_trustpoint
Router(config)# crypto ca import server_root_CA_trustpoint pkcs12 path password
```

Step 3 Configure the authentication method as EAP-TLS:

```
Router# configure terminal
Router(config)# interface wimax interface
Router(config-if)# pkm trustpoint server_root_ca server_root_CA_trustpoint
Router(config-if)# pkm auth-method eap-tls
Router(config-if)# pkm version pkm-v2
Router(config-if)# pkm trustpoint device device_cert_trustpoint <-- *
Router(config-if)# pkm trustpoint server_root_ca
```

> **Note** *—The command, **pkm trustpoint device device_cert_trustpoint**, is not needed if 1) EAP-TLS is using the embedded Airspan certificate, or 2) if EAP-TTLS is used.

Enabling an Interface

To configure a WiMAX interface, issue the following commands:

```
Router# configure terminal
Router(config)# interface wimax 2/1
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

Additional WiMAX Configuration Commands

The following are the WiMAX configuration commands:

- (config)# **wimax scan-list** *scan_list_name*
- (config-scan-list)# **nap id nap-id priority** *priority* **channel-index** *channel-index*
- (config-scan-list)# **nsp id nsp-id** {**home** | **priority** *priority* **channel-index** *channel-index*}
- (config-if)# [**no**] **wimax pkm-version** {**pkm-v2**}
- (config-if)# [**no**] **shutdown**
- (config-if)# [**no**] **ip address** {*IP_address_in_format_i.i.i.i* | *IP_prefix_and_network_mask_length_in_format_x.x.x.x/m IP_network_mask_in_format_m.m.m.m*}

WiMAX show Command Examples

The following are WiMAX related **show** commands:

show sprom

To show the command options for the **show sprom** command, do the following:

```
Router# show sprom ?
  all         Show all sproms contents
  backplane   Show backplane clock module sprom contents
  clock       Show backplane clock module sprom contents
```

```
fan          Show fan module sprom contents
mgmt-module  Show mgmt module (MDS9216/MDS9216i/MDS9222i only) sprom contents
module       Show linecard module sprom contents
powersupply  Show powersupply sprom contents
stby-sup     Show stanby supervisor sprom contents
sup          Show supervisor sprom contents
xbar         Show xbar fabric sprom contents
```

show interfaces wimax *interface_name* association

The following is an example of the **show interfaces wimax** *interface_name* **association** command:

```
Router # show interface wimax 3/1 association
        Interface           : Wimax3/1
        MAC address         : 00a0.0ad2.072f
        Internet Address    : 192.10.0.200/24
        Device name         : Sequans SQN12X0
        Key management      : None
        Authen method       : Open
        Physical layer state : Connected
        Link modulation     : OFDMA
        BSID                : 00:02:AA:00:00:01
        NAP                 : 00:02:AA

        Frequency           : 2310000 kHz
        Channel bandwidth   : 10000 kHz
        TX power            : 6 dBm
        RSSI                : -82 dBm
        CINR                : 20 dB
        Uptime              : 17344 s
        Bytes in            : 790189879
        Packets in          : 722443
        Bytes out           : 790721010
        Packets out         : 621521
```

show controllers wimax *interface_name*

The following is an example of the **show controllers wimax** *interface_name* command:

```
Router # show controllers wimax 6/1
        Interface                        : wimax6/1
        Hardware address                 : 0016.0800.118c
        Service daemon version           : 4.6.2.4-27804
        Kernel driver version            : 4.6.2.4-004
        Firmware version                 : 4.6.2.4-28584
        Microcode version                : 6.7.2.2-8517
        Hardware version                 : 10.7.0.0-8517
        Board version                    : SQN12X0
        Chip version                     : SQN12X0
        RF Chip version                  : SQN12X0
        Minimum frequency                : 2500000
        Maximum Frequency                : 2700000
        current frequency                : 2550000
        Bandwidth                        : 10MHz
        Frame duration                   : 5000
        Attached scan list               : "aaa"
        Min RSSI            -72 dBm
        Min CINR            28 dB
        Min Duration        100 msec
        Min Scan Interval   100 msec
        Max Scan Interval   200 msec
        Retries             5 ?
```

```
          Initial RNG Backoff Start  :      0
          Initial RNG Backoff End    :      5
          Periodic RNG Backoof Start :      0
          Periodic RNG Backoff End   :      3
          Bandwidth Request Backoof Start :      0
          Bandwidth Request Backoff End   :      3
          UL Permutation          :          0
          UL  Subchannel-bitmap   :   0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
          Initial-RNG code qty    :          4
          Periodic-RNG code qty   :          4
          BWR code qty            :          4
          DLC CONFIG:
          bsEirp  (dBm)           :          4.0
          maxRssInitRanging (dBm)     :      0.0
          PHY:
          BSiD                        :0000.000.0000
          Qos Classifiers   :   6
          Qos Connections   :   6
```

show interfaces wimax *interface_name* statistics

The following is an example of the **show interfaces wimax** *interface_name* **statistics** command:

```
Router # show interfaces wimax 2/1 statistics
        WiMAX Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER                           TRANSMITTER
Host Rx K Bytes:     923438 / 24366    Host Tx K Bytes:        115 / 0
Unicasts Rx:              0 / 0        Unicasts Tx:              0 / 0
Unicasts to host:        0 / 0        Unicasts by host:         0 / 0
Broadcasts Rx:       29482 / 734      Broadcasts Tx:            0 / 0

TBD.  Add stats provided by proximetry
```

show interface wimax *interface_name* scanning

The following is an example of the **show interfaces wimax** *interface_name* **scanning** command:

```
Router # show interface wimax 3/1 scanning
Scan results for interface: Wimax3/1

BSID: 00:02:AA:00:00:01
        Frequency: 2310000
        NAPID: 00:02:AA
        RSSI: -82 dBm
        CINR: 20 dB
```

Troubleshooting and Diagnostics

This section provides the necessary background information and resources available for troubleshooting the 2G/3G Connected Grid module.

WiMAX Debug Commands

The following are the WiMAX exec debug commands:

- **clear interface wimax** *interface name* **statistics**
- **debug wimax pm** {**all** | **demux** | **deque** | **error** | **event** | **trace** | **warning**}

Checking Signal Strength

If the Received Signal Strength Indication (RSSI) level is very low (for example, if it is less than -110 dBm), follow these steps:

Step 1 Check the antenna connection. Make sure the TNC connector is correctly threaded and tightened.

Step 2 If you are using a remote antenna, move the antenna cradle and check if the RSSI has improved.

Step 3 Contact your wireless service provider to verify that there is service availability in your area.

Retrieving the Electronic Serial Number

If your network provider requests the 11-digit decimal equivalent of your Electronic Serial Number (ESN), you must retrieve your ESN, then convert it to decimal notation. See also, .

The ESN number is located directly on the modem label in hexadecimal notation. It can also be retrieved using the Cisco IOS CLI using the **show sprom module** *module number slot_number* command.

The sample output below shows the ESN number:

```
Router (config-if)# show sprom module 5 1
DISPLAY linecard sprom contents of module 5:
lc-sprom linecard block header is invalid
cur_blk_hdr->block_length = 0067
cur_blk_hdr->block_signature = 6003
WARNING: sprom contents are invalid for module 5 instance 1
WARNING: please power down the module and program the sprom contents
Common block:
Block Signature : 0xabab
Block Version   : 3
Block Length    : 160
Block Checksum  : 0x1494
EEPROM Size     : 65535
Block Count     : 2
FRU Major Type  : 0x6002
FRU Minor Type  : 0x0
OEM String      : Cisco Systems, Inc.
Product Number  : CALABRIA
Serial Number   : JAF1542AFJQ
Part Number     : 73-13545-01
Part Revision   : 18
Mfg Deviation   : 0
H/W Version     : 0.0
Mfg Bits        : 0
Engineer Use    : 0
```

```
snmpOID         : 0.0.0.0.0.0.0.0
Power Consump   : -189
RMA Code        : 0-0-0-0
CLEI Code       : TESTING123
VID             : V01
Linecard Module specific block:
Block Signature : 0x6003
Block Version   : 2
Block Length    : 103
Block Checksum  : 0x854
Feature Bits    : 0x0
HW Changes Bits : 0x0
Card Index      : 30004
MAC Addresses   : 00-00-00-00-00-00
Number of MACs  : 12
Number of EOBC links : 1
Number of EPLD  : 16
EPLD A          : 0x0
EPLD B          : 0x0
EPLD C          : 0x0
EPLD D          : 0x0
EPLD E          : 0x0
EPLD F          : 0x0
EPLD G          : 0x0
EPLD H          : 0x0
EPLD I          : 0x0
EPLD J          : 0x0
EPLD K          : 0x0
EPLD L          : 0x0
EPLD M          : 0x0
EPLD N          : 0x0
EPLD O          : 0x0
EPLD P          : 0x0
Port Type-Num   : 11-1
SRAM size       : 0
Sensor #1       : 73,60
Sensor #2       : 69,55
Sensor #3       : 77,65
Sensor #4       : 71,60
Sensor #5       : 65,50
Sensor #6       : -128,-128
Sensor #7       : -128,-128
Sensor #8       : -128,-128
Max Connector Power: 1200
Cooling Requirement: 70
Ambient Temperature: 55
...
```

Converting Hexadecimal ESN to Decimal Notation

If your network provider requests the 11-digit decimal equivalent of your Electronic Serial Number (ESN), you must retrieve your ESN, then convert it to decimal notation. See also, Retrieving the Electronic Serial Number, page 24.

To convert the ESN number from hexadecimal notation to decimal notation:

Step 1   Start with the 8-digit HEX ESN # obtained from the label or using CLI, for example 0x603C9854. This number consists of two parts:

- 0x60—Serial number

- 3C9854—Manufacturer's code

Step 2 Convert manufacturer's code to decimal as shown:

- Hexadecimal 0x60 equals decimal 96.

- If the decimal value is two digits only, prepend it with a zero to expand it to three digits.

- Manufacturer's code is thus 096.

Step 3 Convert the serial number to decimal, as shown in the example below:

- Hexadecimal 0x3C9854 equals decimal 3971156.

- If decimal value is less than 8 digits, add enough zeros to make it into an 8 digit number.

- Serial number is thus 03971156.

Step 4 To obtain complete 11-digit decimal ESN notation, combine manufacturer code and serial number:

- Manufacturer code: 096

- Serial #: 03971156

- Decimal ESN: 09603971156

Additional References

Consult the following resources for related information about the WiMAX module or for technical assistance:

- Hardware Overview and Installation Documents, page 26

- Supported Cisco Antennas and Accessories Documents, page 26

- Cisco System Software Commands Documents, page 27

- Regulatory, Compliance, and Safety Information, page 27

Hardware Overview and Installation Documents

- *Cisco Connected Grid Modules*

  http://www.cisco.com/en/US/products/ps10984/prod_module_series_home.html

- *Cisco CGR 1240 Hardware Installation Guide*

  http://www.cisco.com/en/US/docs/routers/connectedgrid/cgr1000/hardware/cgr1240/installation.html

- *Cisco 1000 Series Connected Grid Routers*

  http://www.cisco.com/en/US/partner/products/ps12256/tsd_products_support_series_home.html

Supported Cisco Antennas and Accessories Documents

- Connected Grid Antennas Installation Guide

  http://www.cisco.com/en/US/docs/routers/connectedgrid/antennas/installing/cg_antenna_install_guide.html

- *Lightning Arrestor for the Cisco 1240 Connected Grid Router*

Cisco System Software Commands Documents

- *Cisco Connected Grid Device Manager User Guide*
- *Cisco System Software*

    http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
- *Configuring Cisco EHWIC-3G-EDVO-x*

    http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/mrwls_evdo.html
- *Cisco 1000 Series Connected Grid Routers Unicast Routing Software Configuration Guide*

Regulatory, Compliance, and Safety Information

- Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information

    http://www.cisco.com/en/US/docs/routers/access/interfaces/rcsi/IOHrcsi.html

Feature History

Table 8 provides a feature history for the Cisco connected grid modules for the CGR 1000 Series and WiMAX installation and configuration.

Table 8   Feature history for Cisco Connected Grid Modules for CGR 1000 Series and WiMAX installation and configuration

Feature Name	Release	Feature Information
WiMAX module	Cisco CG-OS Release CG3	The IEEE 802.16e WiMAX module for Cisco CG-OS router provides a WAN interface for communication over WiMAX wireless (1.8 or 2.3GHz) infrastructure in multi-services FAN (Field Area Networks) deployments.
EAP-Tunneled Transport Layer Security (EAP-TTLS) on WiMAX	Cisco CG-OS Release CG3	The WiMAX module supports EAP-TTLS, as defined in RFC 5281. EAP-TTLS allows a client to be authenticated by a server using a secure tunneled connection after the server has been securely authenticated to the client using its CA certificate.
Support for 1.4 and 3.65GHz. bands	Cisco CG-OS Release CG4	Initial support of the bands on the CGR 1000 WiMAX module.

Technical Assistance

The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.

http://www.cisco.com/cisco/web/support/index.html

Tell Us What You Think
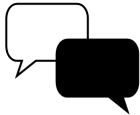
Send your feedback about this document directly to the Connected Energy Documentation Team.

Connected Grid Documentation Feedback Form

This document is to be used in conjunction with the documents listed in the "Additional References" section.